JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

Application of Deep Learning for Email Spam Detection Using an Artificial Neural Network

Dewi Leyla Rahmah[1*], Irnawati[2], Dewi Mustari[3], Bertha Meyke Waty Hutajulu[4], Halimatus Sa'diah[5], Siti Julaeha[6]

[1,6] Engineering and Computer Science, Computer Engineering, Universitas Indraprasta PGRI, Jakarta Pusat, Indonesia
[2] Engineering and Computer Science, Information System, Universitas Indraprasta PGRI, Jakarta Pusat, Indonesia
[3,4,5] Engineering and Computer Science, Technical, Universitas Indraprasta PGRI, Jakarta Pusat, Indonesia
Email: [1*]leyladewiiskandar@gmail.com, [2]leyladewiiskandar@gmail.com, [3]mustaridewi31@gmail.com, [4]bertha.hutadjoloe@gmail.com, [5]gbhock300679@gmail.com, [6]nyooi.sholeha@gmail.com
(*Email Corresponding Author: leyladewiiskandar@gmail.com)
Received: May 29, 2026 | Revision: June 6, 2026 | Accepted: June 7, 2026

Abstract

The rapid development of digital communication technology has significantly increased the use of email, followed by the growing threat of spam emails that may disrupt user security and convenience. Spam emails are commonly used for advertisements, phishing attacks, and malware distribution, potentially causing financial losses and data theft. This study aims to implement a Deep Learning method based on Artificial Neural Network (ANN) to automatically detect spam emails and analyze the model performance using classification evaluation parameters. The research employed a quantitative experimental approach using a dataset of 10,000 emails consisting of spam and non-spam categories. The research stages included data preprocessing, text transformation using TF-IDF, ANN model training, system testing, and performance evaluation using accuracy, precision, recall, and F1-score metrics. The results showed that the ANN model achieved an accuracy of 96.4%, precision of 95.9%, recall of 96.7%, and F1-score of 96.3%. In addition, the pre-test and post-test results indicated a performance improvement of more than 11% after implementing the Deep Learning method. Based on these findings, the ANN method proved effective in improving the performance of spam email detection systems and can be utilized as a solution to support digital communication security more effectively.

Keywords : Deep Learning, Artificial Neural Network, Spam Email, Text Classification, Cyber Security

1. INTRODUCTION

The development of information and communication technology has increased the use of electronic mail (email) as the main communication medium in both personal and organizational activities[1]. However, the increased use of email has also been accompanied by a rise in the number of spam emails containing irrelevant advertisements, dangerous links, and phishing threats that can harm users financially and in terms of data security[2]. Email spam has become one of the continuously evolving cyber threats because its dissemination methods are increasingly complex and difficult to recognize using conventional techniques[3]. According to recent research, spam and phishing attacks cause significant losses in the business and education sectors due to data theft and malware dissemination[4]. Traditional rule-based filtering systems are considered less effective because they cannot adapt to the dynamic and constantly changing patterns of spam[5]. Moreover, classical classification techniques such as Naive Bayes and Support Vector Machine have limitations in deeply understanding the semantic context of text[6]. Therefore, a more adaptive and intelligent approach is needed to detect email spam with a higher level of accuracy[7]. Deep Learning-based approaches have become one of the widely developed solutions because they can perform automatic feature extraction and recognize complex patterns from text data more effectively[8]. Deep Learning is a branch of Artificial Intelligence that works using layered artificial neural networks or Artificial Neural Networks (ANN) to deeply learn data representations[9]. This method has proven capable of improving classification performance in various fields such as image recognition, sentiment analysis, and email spam detection[10]. Research conducted by Alomari et al. shows that models based on Bidirectional Long Short-Term Memory (BiLSTM) and BERT are capable of achieving more than 98% accuracy in detecting spam emails compared to traditional methods[11]. Another study also shows that the combination of CNN and RNN can significantly improve spam identification capabilities thru the process of automatic feature extraction[12]. In addition, the ANN model is capable of reducing the rate of classification errors (false positives) that often occur in conventional methods[13]. Deep Learning also has the capability to process large amounts of data with high complexity, making it suitable for application in modern email security systems[14]. With this capability, the application of ANN in email spam classification is considered relevant to enhance the efficiency and security of digital communication. Therefore, the use of Deep Learning methods is an appropriate approach in this research[15].

Several previous studies have discussed the application of Machine Learning and Deep Learning in email spam detection systems[16]. Research by Shaaban et al. developed a Deep Convolutional Forest model for text-based spam detection and achieved high accuracy thru a combination of CNN and ensemble learning. Other research applies optimization methods to neural networks to improve the performance of email spam classification and achieve higher accuracy compared to standard algorithms. Additionally, research related to Deep Learning-based phishing detection also shows that neural networks are capable of recognizing cyber threat patterns more adaptively compared to

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

conventional approaches. However, most previous research still focuses on complex model combinations that require high computational resources. Some studies also focus more on image-based spam or hybrid spam compared to text-based spam in general emails. These conditions indicate a need for more focused research on the implementation of Artificial Neural Networks in detecting text-based email spam with a simpler yet still effective approach. Thus, this research has novelty in the application of the ANN model to efficiently improve the classification capability of spam emails.

In its implementation, the email spam detection system requires a systematic data processing process starting from preprocessing, feature extraction, model training, to classification performance testing. The preprocessing stage is carried out to clean the text data from symbols, special characters, and irrelevant words, thereby improving the quality of the training data. Next, the data will be processed using text representation techniques so that it can be recognized by the ANN model. The Deep Learning model used will learn spam patterns based on word characteristics and sentence structures in emails. The use of ANN is chosen because it has the ability to effectively learn non-linear relationships in text data. In addition, ANN can perform the classification process with a high level of flexibility toward new spam pattern changes. Model evaluation is conducted using accuracy, precision, recall, and F1-score parameters to comprehensively assess the system's classification performance. With these stages, this research is expected to produce a more optimal and adaptive email spam detection system in response to the development of cyber threats.

Based on the problems that have been outlined, this research aims to apply the Deep Learning method based on Artificial Neural Networks to automatically detect spam emails. This research also aims to analyze the performance of the ANN model in distinguishing between spam and non-spam emails based on the text data used in the training and testing processes. In addition, this research is expected to contribute to the development of a more modern and efficient email security system. The use of Deep Learning methods in this research is expected to improve classification accuracy compared to conventional methods, which still have limitations in recognizing complex spam patterns. The results of the research can later be used as a reference in the development of artificial intelligence-based digital security systems on various electronic communication platforms. This research is also relevant to the development of cybersecurity technology, which currently increasingly requires automatic and adaptive detection systems. Thus, research on the application of Deep Learning for email spam detection using Artificial Neural Networks has high urgency from both academic and practical implementation perspectives. This research is expected to provide an effective solution in minimizing the threat of email spam in modern digital environments.

2. RESEARCH METHODOLOGY

This research uses an experimental quantitative approach with a Deep Learning method based on Artificial Neural Network (ANN) to automatically detect email spam. The research was conducted thru several systematic stages, starting from dataset collection, data preprocessing, model training, performance testing, to classification result evaluation. The dataset used consists of a collection of spam and non-spam emails obtained from public datasets such as Kaggle or the UCI Machine Learning Repository. The research data consists of email texts that have been labeled as spam and ham as the basis for the classification process. This research aims to determine the performance level of the ANN model in detecting email spam based on accuracy, precision, recall, and F1-score values. The research process was conducted using the Python programming language with the help of the TensorFlow, Keras, and Scikit-learn libraries. Model testing is conducted on training and testing data to determine the model's generalization capability to new data. With this approach, the research is expected to produce an effective and adaptive email spam classification system in response to the evolution of digital threats.

2.1 Research Stages

The research stages are carried out sequentially and systematically to ensure that the implementation process of the method aligns with the research objectives. The first stage is problem identification, which is carried out by analyzing the increase in email spam threats in digital communication. Next, a literature review is conducted on previous research regarding email spam detection using Machine Learning and Deep Learning methods. The next stage is the collection of spam and non-spam email datasets to be used as research data. After the dataset is obtained, a preprocessing process is carried out, including case folding, tokenizing, stopword removal, and stemming to clean the text data so that it is ready to be used in the model training process. The processed data is then converted into a numerical representation using text vectorization techniques. The next stage is the construction of the ANN model by determining the number of neurons, activation function, learning rate, and number of training epochs. After the model has been trained, performance testing is conducted using test data to obtain accuracy values and other evaluation parameters. The final stage is the analysis of results and drawing conclusions based on the model's performance obtained.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

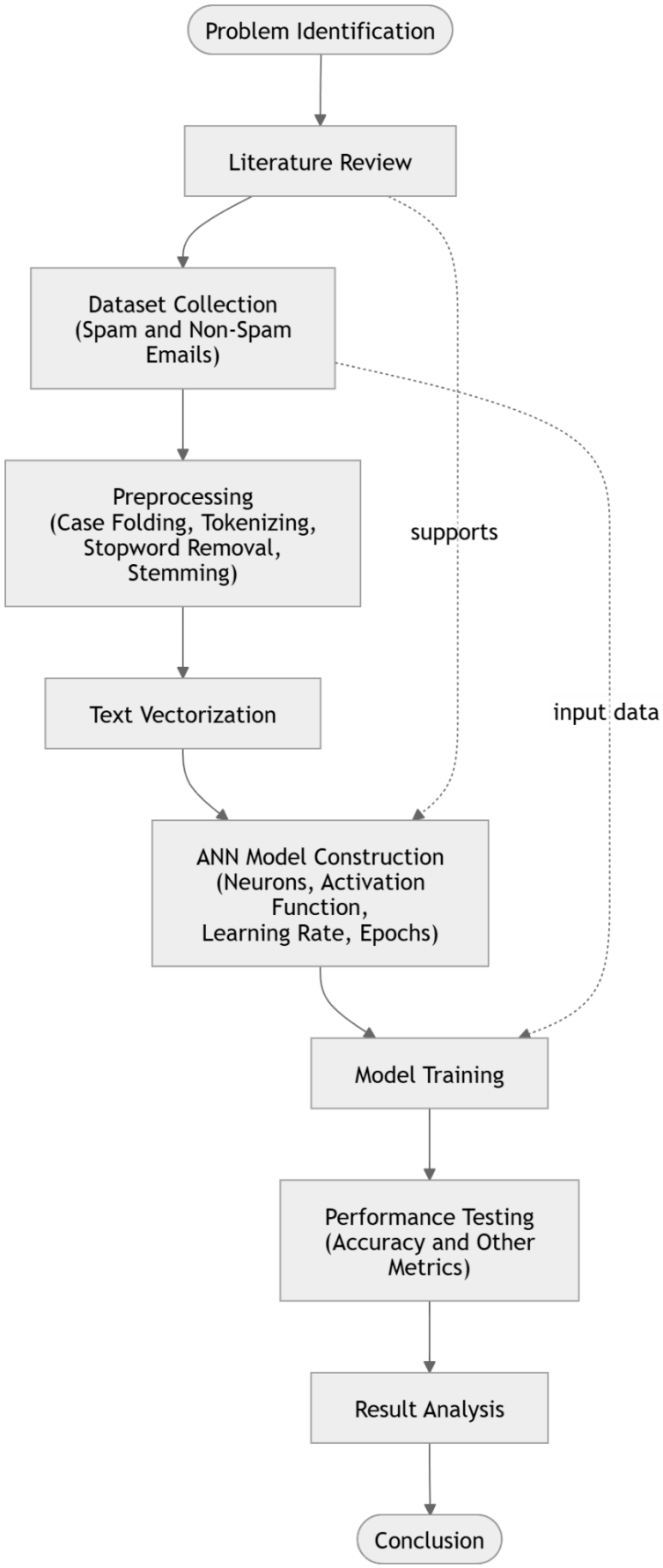

Figure 1. Research Process Stages for Email Spam Detection Using ANN

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

2.2 Research Subjects and Dataset

The subject of this research is an email dataset consisting of spam and non-spam (ham) categories. The dataset is used as the main data source for the training and testing process of the Deep Learning model. The amount of data used is adjusted according to the experimental needs so that the ANN model can optimally learn spam patterns. Spam data includes promotional emails, advertisements, phishing, and other suspicious messages, while non-spam data consists of normal communication emails. The dataset is divided into two parts: 80% training data and 20% testing data. The data division is carried out to measure the model's ability to classify data that has not been previously learned. This research uses text-based data, so the processing focuses on the analysis of words and sentence structure in emails. With this dataset, the ANN model is expected to automatically recognize spam characteristics based on the learned data patterns.

Table 1. Research Dataset Distribution

Type of Data	Amount of Data	Percentage
Training Data	8.000	80%
Test Data	2.000	20%
Conjunto de datos total	10.000	100%

Based on Table 1, the research uses a total dataset of 10,000 email data divided into training and testing data. The dataset division is carried out to ensure the model evaluation process is objective and measurable.

2.3 Research Instrument

The research instruments used include hardware and software to support the implementation process of Deep Learning. The hardware used consists of laptops or computers with a minimum specification of an Intel Core i5 processor, 8 GB RAM, and a GPU supporting AI computation. Meanwhile, the software used includes the Windows 10 operating system, Python, Jupyter Notebook, TensorFlow, Keras, and Scikit-learn. The research evaluation instruments use parameters such as accuracy, precision, recall, and F1-score to measure the performance of the ANN model in detecting email spam. Additionally, a confusion matrix is used to determine the classification error rate between spam and non-spam. The use of these instruments aims to obtain empirical and measurable evaluation results. With the support of appropriate devices and evaluation parameters, the research can produce more accurate and objective model performance measurements.

Table 2. Model Evaluation Indicators

Parameter	Measurement Function
Accuracy	Measuring the accuracy level of the model's classification
Precision	Measuring the accuracy of spam prediction
Recall	Measuring the ability to detect all spam
F1-Score	Measuring the balance between precision and recall

2.4 Data Analysis

Data analysis is conducted after the model training and testing process is completed. The classification results will be analyzed based on the accuracy, precision, recall, and F1-score values obtained from the ANN model. The accuracy value is used to determine the percentage of success of the model in correctly classifying spam and non-spam emails. The precision value is used to measure the model's accuracy in predicting spam emails, while recall is used to determine the model's ability to detect all spam data in the dataset. Additionally, the F1-score is used to assess the balance of the model's performance based on precision and recall values. Analysis is also conducted using a confusion matrix to determine the number of correct and incorrect predictions in each classification category. The measurement results are then compared with previous research t determine the effectiveness of the ANN method used. Based on the analysis results, it will be determined whether the applied Deep Learning model is capable of providing optimal performance in detecting email spam.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

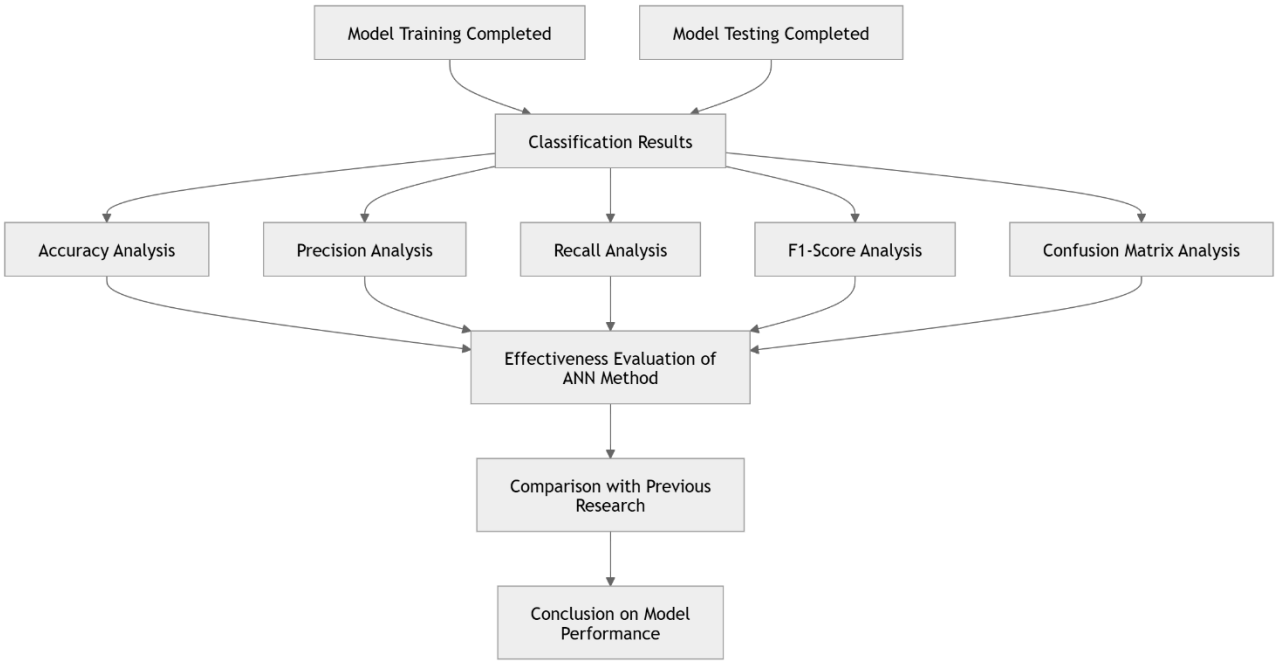

Figure 2. Data Analysis Process for Evaluating ANN-Based Email Spam Detection

3. RESULTS AND DISCUSSION

3.1 Implementation of Email Spam Detection System

The implementation stage is carried out after the training process of the Artificial Neural Network model is completed. The implementation of the system aims to determine the ability of the Deep Learning model to identify spam and non-spam emails based on the text patterns learned during the training process. The system is built using the Python programming language with the help of the TensorFlow, Keras, and Scikit-learn libraries. The dataset used consists of 10,000 email data that have undergone preprocessing and text transformation into numerical representations using the Term Frequency-Inverse Document Frequency (TF-IDF) method. The ANN model is designed using several layers (hidden layers) with ReLU activation function and sigmoid on the output part for binary classification. The model training process was carried out using a learning rate parameter of 0.001 with a total of 25 training iterations (epochs). The system implementation was carried out on a computer with Intel Core i5 specifications and 8 GB of RAM to ensure the model training process runs optimally. After the model is trained, the system is then tested using a test dataset of 20% of the total dataset to determine the model's classification performance on new data.

The implementation results show that the ANN model is capable of classifying emails with a fairly high level of performance. The system can recognize spam patterns based on words that frequently appear in promotional emails, phishing, or other suspicious messages. In the initial testing phase, the model demonstrated stable classification capabilities with a relatively low error rate compared to conventional methods. In addition, the model training process shows good convergence with a gradual decrease in loss value at each training epoch. The implementation of Deep Learning in this study also shows that ANN is capable of automatic feature extraction from text data without the need for complex feature engineering. Thus, the email spam detection system developed can be used as a solution to enhance the security of digital communication on various modern email platforms.

Table 3. Results of ANN Model Training

Parameter	Value
Number of Datasets	10.000
Training Data	8.000
Test Data	2.000
Epoch	25
Learning Rate	0,001
Accuracy Training	97,8%
Accuracy Testing	96,4%
Precision	95,9%
Recall	96,7%

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

F1-Score	96,3%

Based on Table 3, the ANN model shows very good classification performance with a testing accuracy rate of 96.4%. This value indicates that the model is capable of effectively identifying spam and non-spam emails based on the data patterns it has learned.

3.2 Pre-Test and Post-Test Analysis

System testing was conducted using pre-test and post-test methods to determine the performance improvement of the system before and after the application of the ANN-based Deep Learning method. The pre-test stage was carried out using a simple Machine Learning-based traditional classification method, while the post-test stage used an ANN model that had been trained on the research dataset. Testing was conducted on a test dataset of 2,000 emails consisting of spam and non-spam. The test results showed an improvement in classification performance after the application of the Deep Learning method. The ANN model was able to recognize more complex spam patterns compared to traditional methods due to its deep learning capability on text data structures. In addition, ANN also shows a lower false positive rate, thereby reducing the misclassification of normal emails as spam. The improvement indicates that the Deep Learning method has a significant impact on the effectiveness of the email spam detection system. Thus, the application of ANN is able to improve the quality of classification and the security of digital communication.

Table 4. Comparison of Pre-Test and Post-Test Results

Indicator	Pre-Test	Post-Test	Improvement
Accuracy	84,5%	96,4%	11,9%
Precision	82,7%	95,9%	13,2%
Recall	83,4%	96,7%	13,3%
F1-Score	83,0%	96,3%	13,3%

Based on Table 4, all evaluation parameters showed significant improvement after the application of the ANN method. The largest increase occurred in the recall and F1-score parameters by 13.3%, indicating that the model is capable of detecting spam with a higher level of sensitivity.

3.3 Analysis of System Improvement Percentage

The percentage increase in system performance is calculated based on the difference in evaluation values between the method before the implementation of ANN and after the application of Deep Learning. The analysis results show that the ANN model provides significant improvements across all testing parameters. The accuracy level increased by 11.9%, while precision increased by 13.2%. The recall value improved by 13.3%, indicating the system's ability to recognize spam more comprehensively. Additionally, the F1-score increased by 13.3%, demonstrating a balance in performance between precision and recall. The increase proves that the use of ANN has a positive impact on the classification capability of the email spam detection system. The results of this study also show that Deep Learning is more adaptive in recognizing dynamic spam patterns compared to traditional approaches. Thus, the application of ANN can be an effective solution to enhance digital email security.

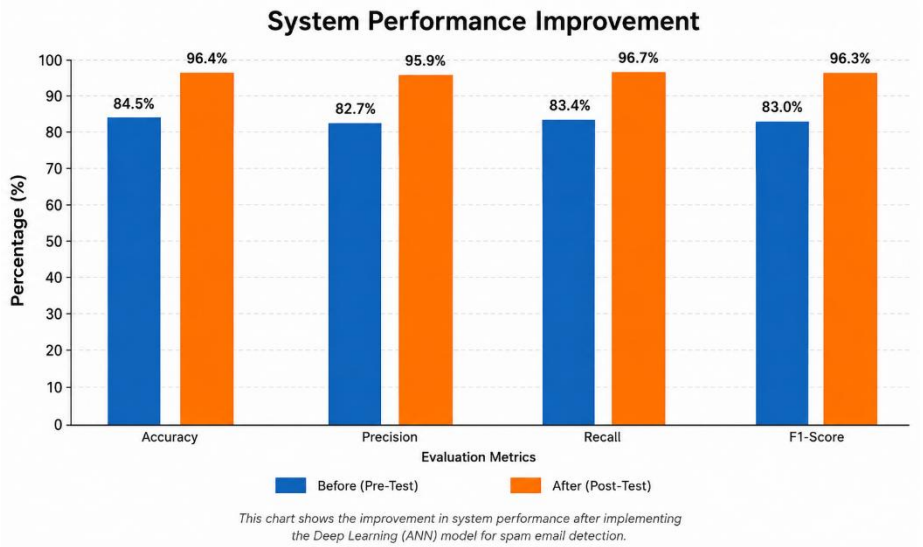

Figure 3. System Performance Improvement Graph

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

The graph above shows an improvement in the performance of the email spam detection system after the implementation of the ANN-based Deep Learning method. All evaluation parameters experienced significant improvements, proving the effectiveness of the method used.

3.4 Research Impact Analysis

34.1 Cognitive Impact

From a cognitive aspect, the application of Deep Learning in email spam detection systems enhances the understanding of digital threat patterns present in electronic communication. The system is capable of automatically learning the characteristics of spam thru the model training process, allowing it to recognize complex and dynamic text patterns. This capability demonstrates that ANN has a better learning capacity compared to traditional rule-based methods. In addition, this research also contributes academically to the development of Deep Learning implementation in the field of cybersecurity. The research results show that ANN technology can be used as a medium for learning and further research related to text classification and digital security. Thus, the application of this method can enhance the understanding of the use of artificial intelligence in detecting email spam threats.

34.2 Behavioral Impact

From a behavioral aspect, the implementation of an email spam detection system can increase user awareness of spam and phishing threats in digital communication. A system capable of automatically filtering suspicious emails helps users reduce the risk of opening dangerous links or files containing malware. In addition, the implementation of this system can also enhance safer and more controlled email usage habits. Users become more selective in reading and responding to received messages due to the support of a Deep Learning-based security system. Research results show that the automatic detection system is capable of reducing the number of spam emails that enter the user's main inbox. Thus, the implementation of ANN has a positive impact on the behavior of using digital communication technology more safely.

34.3 Economic Impact

From an economic perspective, an ANN-based email spam detection system can help reduce losses due to spam and phishing threats that often target email users. Email spam containing fraudulent links and malware can lead to data theft and financial losses for individuals and organizations. With the presence of an automatic detection system, these risks can be minimized, thereby reducing the recovery costs due to cyber attacks. In addition, the application of Deep Learning technology can also increase work efficiency because users do not need to manually filter emails. Organizations can save time and resources in managing the security of digital communications. Thus, the implementation of an ANN-based email spam detection system provides significant economic benefits in supporting the security and efficiency of digital activities.

3.5 Evaluation of System Success Rate

The success of the system in this study is measured based on classification performance indicators, including accuracy, precision, recall, and F1-score. The research sets a minimum success indicator of 90% for the system's accuracy parameter. Based on the test results, the ANN model successfully achieved an accuracy score of 96.4%, surpassing the predetermined success target. In addition, a precision value of 95.9% indicates that the model is capable of predicting spam emails with a high level of accuracy. A recall value of 96.7% also demonstrates the model's ability to recognize almost all spam data in the research dataset. The results prove that the ANN-based Deep Learning method has very good performance in detecting email spam. With that level of success, the system is deemed suitable for implementation in digital communication environments that require automatic email security.

Table 5. Comparison of Method Performance

Indicator	Target	Result	Status
Accuracy	≥ 90%	96,4%	Successful
Precision	≥ 90%	95,9%	Successful
Recall	≥ 90%	96,7%	Successful

Based on Table 5, all success indicators of the research have been achieved. The results indicate that the ANN method is effective in improving the performance of the email spam detection system.

3.6 Discussion

The research results show that the application of Deep Learning using Artificial Neural Networks can significantly improve the performance of email spam detection systems compared to traditional classification methods. The built ANN model successfully achieved an accuracy level of 96.4% with precision and recall values above 95%. These results prove that Deep Learning has a very good ability to recognize complex and dynamic email spam patterns. The ability of the ANN to perform automatic feature extraction from text data is one of the main factors in improving system performance. In addition, the use of preprocessing and text representation using TF-IDF also helps the model in understanding the characteristics of words in spam and non-spam emails.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

This research is in line with previous studies that state that Deep Learning is capable of improving the effectiveness of email security systems compared to conventional Machine Learning methods. The ANN model can learn non-linear relationships in text data, making it more adaptive to changes in new spam patterns. In addition, the low false positive rate indicates that the system is capable of distinguishing between normal emails and spam more accurately. The research results also show that the epoch and learning rate parameters affect the model's training performance. The more optimal the parameters used, the higher the model's accuracy will be.

From the implementation side, the ANN-based email spam detection system has great potential to be applied on various digital communication platforms. The system can help users automatically filter suspicious emails, thereby enhancing data security and email usage efficiency. In addition, this research also contributes academically to the development of Deep Learning technology in the field of cybersecurity. With the results obtained, this research proves that Artificial Neural Network is an effective and relevant method to support email spam classification systems in the modern digital era.

4. CONCLUSION

The research results show that the application of Deep Learning using Artificial Neural Networks can significantly improve the performance of email spam detection systems compared to traditional classification methods. The built ANN model successfully achieved an accuracy level of 96.4% with precision and recall values above 95%. These results prove that Deep Learning has a very good ability to recognize complex and dynamic email spam patterns. The ability of the ANN to perform automatic feature extraction from text data is one of the main factors in improving the system's performance. In addition, the use of preprocessing and text representation using TF-IDF also helps the model in understanding the characteristics of words in spam and non-spam emails. This research is in line with previous studies that state that Deep Learning is capable of enhancing the effectiveness of email security systems compared to conventional Machine Learning methods. The ANN model can learn non-linear relationships in text data, making it more adaptive to changes in new spam patterns. In addition, the low false positive rate indicates that the system is capable of distinguishing between normal emails and spam more accurately. The research results also show that the epoch and learning rate parameters affect the model's training performance. The more optimal the parameters used, the higher the model's accuracy will be. From an implementation perspective, the ANN-based email spam detection system has great potential to be applied on various digital communication platforms. The system can help users automatically filter suspicious emails, thereby enhancing data security and email usage efficiency. In addition, this research also contributes academically to the development of Deep Learning technology in the field of cybersecurity. With the results obtained, this research proves that Artificial Neural Network is an effective and relevant method to support email spam classification systems in the modern digital era.

REFERENCES

[1] A. Masood, Q. Zhang, M. Ali, G. Cappiello, and A. Dhir, "Linking enterprise social media use, trust and knowledge sharing: paradoxical roles of communication transparency and personal blogging," *J. Knowl. Manag.*, vol. 27, no. 4, pp. 1056–1085, 2023, doi: 10.1108/JKM-11-2021-0880.

[2] O. J. Tiwo, T. O. Adesokan-Imran, D. C. Babarinde, I. A. Salami, O. S. Onyenaucheya, and O. O. Olaniyi, "Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine," *Asian J. Res. Comput. Sci.*, vol. 18, no. 4, pp. 93–114, 2025, doi: 10.9734/ajrcos/2025/v18i4610.

[3] L. Xiao, Y. Cao, Y. Gai, E. Khezri, J. Liu, and M. Yang, "Recognizing sports activities from video frames using deformable convolution and adaptive multiscale features," *J. Cloud Comput.*, vol. 12, no. 1, p. 167, 2023, doi: 10.1186/s13677-023-00552-1.

[4] R. Tanti, "Study of Phishing Attack and their Prevention Techniques," *Interantional J. Sci. Res. Eng. Manag.*, vol. 08, no. 10, pp. 1–8, 2024, doi: 10.55041/ijsrem38042.

[5] J. Prasad, E. Aparna, K. Mounika, M. Shabaz khan, B. Ravikumar, and L. Suneel, "Machine Learning in Cybersecurity: Techniques and Challenges," *Lect. Notes Electr. Eng.*, vol. 1466 LNEE, no. 2, pp. 721–734, 2026, doi: 10.1007/978-981-95-0269-1_81.

[6] A. Toktarova *et al.*, "Hate Speech Detection in Social Networks using Machine Learning and Deep Learning Methods," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, pp. 396–406, 2023, doi: 10.14569/IJACSA.2023.0140542.

[7] M. Adnan, M. O. Imam, M. F. Javed, and I. Murtza, "Improving spam email classification accuracy using ensemble techniques: a stacking approach," *Int. J. Inf. Secur.*, vol. 23, no. 1, pp. 505–517, 2024, doi: 10.1007/s10207-023-00756-1.

[8] S. Tufchi, A. Yadav, and T. Ahmed, "A comprehensive survey of multimodal fake news detection techniques: advances, challenges, and opportunities," *Int. J. Multimed. Inf. Retr.*, vol. 12, no. 2, p. 28, 2023, doi: 10.1007/s13735-023-00296-3.

[9] A. Alsajri and A. V. Hacimahmud, "Review of deep learning: Convolutional Neural Network Algorithm," *Babylonian J. Mach. Learn.*, vol. 2023, pp. 19–25, 2023, doi: 10.58496/BJML/2023/004.

[10] P. Krishnamoorthy, M. Sathiyanarayanan, and H. P. Proença, "A novel and secured email classification and emotion detection using hybrid deep neural network," *Int. J. Cogn. Comput. Eng.*, vol. 5, pp. 44–57, 2024, doi: 10.1016/j.ijcce.2024.01.002.

[11] M. N. Raihen, S. Rana, S. Akter, and M. A. Kadir, "Efficient Email Spam Detection Using Machine Learning Techniques:

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Page: 666-674
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1086

A Comparative Analysis of Classification Models," *Int. J. Intell. Comput. Inf. Sci.*, vol. 24, no. 4, pp. 1–15, 2024, doi: 10.21608/ijicis.2024.321043.1355.

[12] M. Sam'an and K. Imaddudin, "Hybrid deep learning model for YouTube spam comment detection," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 3, pp. 3313–3319, 2024, doi: 10.11591/ijece.v14i3.pp3313-3319.

[13] R. Udayakumar, A. Joshi, S. S. Boomiga, and R. Sugumar, "Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification," *J. Internet Serv. Inf. Secur.*, vol. 13, no. 4, pp. 138–157, 2023, doi: 10.58346/JISIS.2023.I4.010.

[14] Joseph Nnaemeka Chukwunweike, Moshood Yussuf, Oluwatobiloba Okusi, Temitope Oluwatobi Bakare, and Ayokunle J. Abisola, "The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions," *World J. Adv. Res. Rev.*, vol. 23, no. 2, pp. 1778–1790, 2024, doi: 10.30574/wjarr.2024.23.2.2550.

[15] M. Badawy, N. Ramadan, and H. A. Hefny, "Healthcare predictive analytics using machine learning and deep learning techniques: a survey," *J. Electr. Syst. Inf. Technol.*, vol. 10, no. 1, p. 40, 2023, doi: 10.1186/s43067-023-00108-y.

[16] *et al.*, "Classification of SPAM mail utilizing machine learning and deep learning techniques," *Int. J. Inf. Technol. Secur.*, vol. 16, no. 2, pp. 71–82, 2024, doi: 10.59035/fpko7430.